NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

DEVELOPING A CONCEPTUAL UNMANNED AERIAL VEHICLE COMMUNICATIONS MOBILE AD HOC NETWORK SIMULATION MODEL

By

Henry L. Blackshear Jr.

June 2002

Thesis Advisor: Alex Bordetsky
Associate Advisor: Isaac Kaminer

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 2002	Master's Thesis

4. TITLE AND SUBTITLE
DEVELOPING A CONCEPTUAL UNMANNED AERIAL VEHICLE COMMUNICATIONS MOBILE AD HOC NETWORK SIMULATION MODEL

5. FUNDING NUMBERS

6. AUTHOR (S)
Blackshear, Jr. Henry L.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the U.S. Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

A growing demand for increased networking interoperability has spawned a requirement for ad hoc networking. One proposal to satisfy the need is development of Unmanned Aerial Vehicle (UAV) communications Mobile Ad Hoc Networks (MANET). In order to establish these UAV MANETs, a large set of Internet Protocol (IP) based routing protocols must be analyzed to determine suitability for incorporation into the UAV MANET. This thesis represents the initial phase in developing a simulation model to look at routing performance parameters for the conceptual UAV MANET. The Optimum Network Performance (OPNET) simulation software tool was used for this analysis. Analysis and simulations of the Ad Hoc On-Demand Vector Protocol (AODV), Dynamic Source Routing protocol (DSR), and Zone Routing Protocol (ZRP) were conducted to determine their suitability for the UAV MANET model. Results conclude that some routing protocols are more suitable for military operations than others and that development of MANET gateway models are required. Additionally, network management and security issues for this conceptual network are addressed.

14. SUBJECT TERMS
Optimum Network Performance simulation tool, OPNET, Zone Routing Protocol, ZRP, Mobile Ad Hoc Networks, MANET, Unmanned Aerial Vehicle, UAV, Ad Hoc On-Demand Vector Protocol, AODV, Dynamic Source Routing protocol DSR, thesis, NPS, Naval Postgraduate School

15. NUMBER OF PAGES 61

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 **Standard Form 298 (Rev. 2-89)**
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DEVELOPING A CONCEPTUAL UNMANNED AERIAL VEHICLE COMMUNICATIONS MOBILE AD HOC NETWORK SIMULATION MODEL

Henry L. Blackshear Jr.
Captain, United States Marine Corps
B.S., University of Maryland University College, 1994

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
June 2002

Author: Henry L. Blackshear Jr.

Approved by: Alex Bordetsky, Thesis Advisor

Isaac Kaminer, Associate Advisor

Dan C. Boger, Chairman
Department of C4I Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

A growing demand for increased networking interoperability has spawned a requirement for ad hoc networking. One proposal to satisfy the need is development of Unmanned Aerial Vehicle (UAV) communications Mobile Ad Hoc Networks (MANET). In order to establish these UAV MANETs, a large set of Internet Protocol (IP) based routing protocols must be analyzed to determine suitability for incorporation into the UAV MANET.

This thesis represents the initial phase in developing a simulation model to look at routing performance parameters for the conceptual UAV MANET. The Optimum Network Performance (OPNET) simulation software tool was used for this analysis. Analysis and simulations of the Ad Hoc On-Demand Vector Protocol (AODV), Dynamic Source Routing protocol (DSR), and Zone Routing Protocol (ZRP) were conducted to determine their suitability for the UAV MANET model. Results conclude that some routing protocols are more suitable for military operations than others and that development of MANET gateway models are required. Additionally, network management and security issues for this conceptual network are addressed.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

First and foremost, I want to express my deepest gratitude to my wife and daughters (Denise, Brittani and Brianna) for their understanding and continued support during the course of my studies and thesis work at the Naval Postgraduate School. Secondly, I want to thank my thesis advisor, Professor Alex Bordetsky, for his superb advice and mentorship. Finally, I would like to give special thanks to my thesis associate advisor, Professor Isaac Kaminer, and my colleague, Veniamin Bourakov, for the support they have provided.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

In the U.S. Naval Institute Proceedings Vice Admiral A.K. Cebrowski outlines how military operations increasingly will capitalize on the advances and advantages of information technology. He specifies, "The shift from platform to network is what enables the more flexible and more dynamic network-centric operation. Therefore, the construction of high-quality networks is top priority." [Ref. 1] As the military continues into the new century it must take full advantage of network-centric warfare. A major player in acquiring speed of command is a well-coordinated Command, Control, Communications, and Intelligence (C4I) infrastructure.

As world events unfold, today's military must be highly mobile and well connected in order to effectively accomplish a myriad of global tasks. Amphibious Readiness Groups (ARG) and Marine Expeditionary Units (MEU) are prime candidates for the forces required to handle these global tasks. However, by the very nature of their missions, they are often given a difficult task of maintaining a geographical C4I. The Navy and Marine Corps have published several concept papers that are intended to focus the naval forces toward missions in the 21st century. By examining a portion of those concepts, it can be seen that Mobile Ad Hoc Networking (MANET) is a critical link to reaching those goals.

1) Strategy 21

"…Marines are prepared to deploy into diverse, austere, and chaotic environments on short notice and accomplish assigned missions **using our unique command, control, and logistic capabilities to operate independently of existing infrastructure.** These unique capabilities allow Marine units to enable joint, allied, and coalition operations…" [Ref. 2]

2) Forward…From the Sea

"…In peacetime U.S. naval forces build interoperability—the ability to operate in concert with friendly and allied forces—so that in the future we can easily participate fully as part of a formal multinational response or as part of **"ad hoc"** coalitions forged to react to short-notice crisis situations. Focusing on the littoral area, Navy and Marine Corps forces can seize and defend advanced bases--ports and airfields—to enable the flow of land-based air and ground forces, while providing the necessary command and control for all joint and allied forces…" [Ref. 3]

The above concepts are dependant on a C4I that is fluid, responsive and networked. One possible method of establishing a well-coordinated C4I infrastructure is through the use of stratospheric networks, but fundamental networking issues remain unsolved. Networks of this manner will be distributive, self-organizing and wireless, which involve many complex communications mechanisms and protocols.

B. PURPOSE

The C4I infrastructure forms the foundation of unity and speed of command that is vital to the conduct of military operations. In a time when short-notice crisis situations are arising; ad hoc coalitions are forming;

unique command, control, and logistic capabilities to operate independently of existing infrastructure are required; and satellite communications are limited, the Department of Defense (DoD) needs every possible technological advantage imaginable to ensure enhanced interoperability. With this in mind, DoD has initiated an acquisition program to develop a family of radios whose functions include certain enhanced IP services and voice/data multiplexing capabilities. The Joint Tactical Radio System (JTRS) program is DoD's effort to acquire a family of affordable, high capacity tactical radios that offer today's warfighter end-to-end communications capabilities. One of the objectives of this program will be operation in a mobile ad hoc networking environment.

The requirement for ad hoc networking has spawned the development of a large set of **IP-based** routing protocols to meet these challenges. No standard has been adopted yet, but some promising protocols are enthusiastically under study. Once a standard is adopted, that adopted protocol can be used to create rapid communications networks. Those networks can be connected and broadened via Unmanned Aerial Vehicle (UAV) communications nodes. The concept of establishing an ad hoc communications network with UAV's will give our forces one more edge to build interoperability.

C. SCOPE

The scope of this thesis is to develop the foundation for simulation modeling of ad hoc routing protocols for use in developing UAV communication simulation models using the Optimum Network Performance (OPNET) simulation software

tool. Additionally, some other issues for consideration in developing a UAV communications network will be identified. The focus will be an analysis of various mobile ad hoc network (MANET) routing protocols that can aid in establishing the UAV communications network. This research is intended to aid Naval and Marine Corps network development, using UAV's as communications nodes for MANET's. All considerations will be based on operations associated with an Amphibious Readiness Group (ARG) and a Marine Expeditionary Unit (MEU).

II. UNMANNED AERIAL VEHICLE NETWORK CONCEPT

A. INTRODUCTION

Today's communications environment has a growing need for increased bandwidth, more satellite services, and enriched transmission capability at cheaper costs. An up and coming idea to help with this situation is the use of airborne communications nodes (ACN). These platforms will orbit at a high altitude for the purpose of relaying wireless services. Not only will these platforms be able to route for ground stations, but will provide a better link to satellites because of its higher altitude location. This concept seems very equitable for business, and can also be applied to military operations.

B. HIGH ALTITUDE LONG ENDURANCE (HALE) PLATFORM

The concept of placing communications on HALE platforms in the stratosphere is ever growing. The stratospheric region of interest extends from about 39,500 ft to just below 100,000 ft. In a military environment, this altitude provides added security for UAV flight operations from enemy observation and retaliation. Of note, communications can be performed at a lower altitude (i.e. 25,000 ft - ideal for the 'Predator' UAV operations); however, most studies have focused toward the higher altitudes. Several platforms for UAV operations are under consideration, but the most popular for the military is the Global Hawk (capable of operating at 65,000ft).

The Air Force has begun the study of using Global Hawk as an ACN and has looked into some payload, flight, and

frequency parameters. The below information was obtain from a notional mission profile brief of Global Hawk as an ACN: [Ref. 4]

Loiter Altitude:	65,000 Ft for at least 24 hours
Ingress/Egress:	300 NM
Climb/Descent:	200 NM
Runway clearance:	5000 Ft
Sensor Coverage:	40,000 NM^2
Communications:	VHF/UHF voice
	UHF (SATCOM and LOS)
	X-Band (LOS)
	KU-Band (SATCOM)

With research geared toward the extended use of UAVs, the Navy/Marine Corps must capitalize on these efforts and adapt this technology for their use. Two fellow NPS students researched HALE platforms for tactical wireless communications and concluded the following: [Ref. 5]

- The future war fighting doctrines cannot be effectively implemented, either fiscally or technologically, without capabilities that HALE type platforms provide. The stratosphere offers unmatched niche capabilities in many mission areas.
- The Global Hawk offers the most feasible option in HALE capabilities for communication.
- HALE platforms are particularly useful to operations at sea and in littorals.
- The freedom of movement through international airspace and lack of terrain obstruction enable maximum effectiveness of stratospheric platforms.

C. CONCEPT OF OPERATIONS

Once UAVs are flying as communications nodes, another step toward implementing this technology into the

Navy/Marine Corps' mission must take place. The UAVs must be fitted with a communications routing capability that adapts to the specific nature of amphibious operations. The network of UAVs can be controlled from an Amphibious Ship or a Marine Ground unit. The quantity of UAVs in a particular network is dependant on the size of the battle area. A UAV communications network is flexible and can be established as soon as rapid deployable units require. The UAV network will be able to link vital sub-networks in the battle area and provide a capability for information to be passed from Commanding Generals directly down to a Marine squad. This concept will be accomplished with the aid of routing algorithms that are designed for MANET operations.

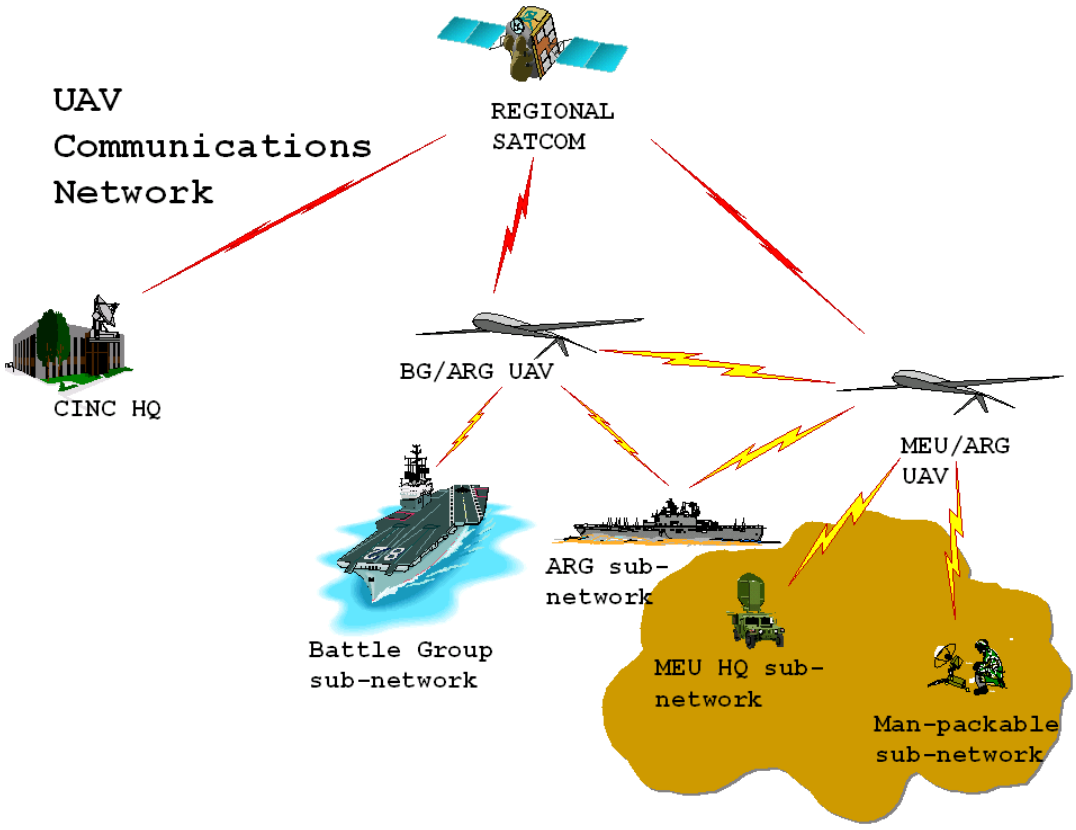


Figure 1. UAV Communications Network

D. NETWORK TOPOLOGY

The proposed network topology is simple. Once a UAV has been equipped with ad hoc routing capabilities, it can link operational networks, as shown in Figure 1. But before this infrastructure can be established, a lot of research must be conducted. The thesis is part of the intended research to develop the UAV architecture. The focus is on profiling mobile ad hoc network routing protocols in order to create a fully functional OPNET simulation model.

III. MOBILE AD HOC NETWORK (MANET) BACKGROUND

A. INTRODUCTION

A MANET is defined as a collection of mobile platforms where each node is free to move about arbitrarily and still be able to communicate with another node that is out of radio range and several routing hops away. Figure 2 shows the differences between MANETs and other traditional network infrastructures (Note that nodes may be connected to other networks). Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. In a MANET, each node logically consists of a router that may have multiple hosts and that also may have multiple wireless communication devices. A MANET can expand an ad hoc wireless network to reach virtually any supported network. One of the original motivations for MANETs is found in the military need for battlefield survivability, operations without pre-placed infrastructure, and connectivity beyond Line-of-Sight. [Ref. 6]

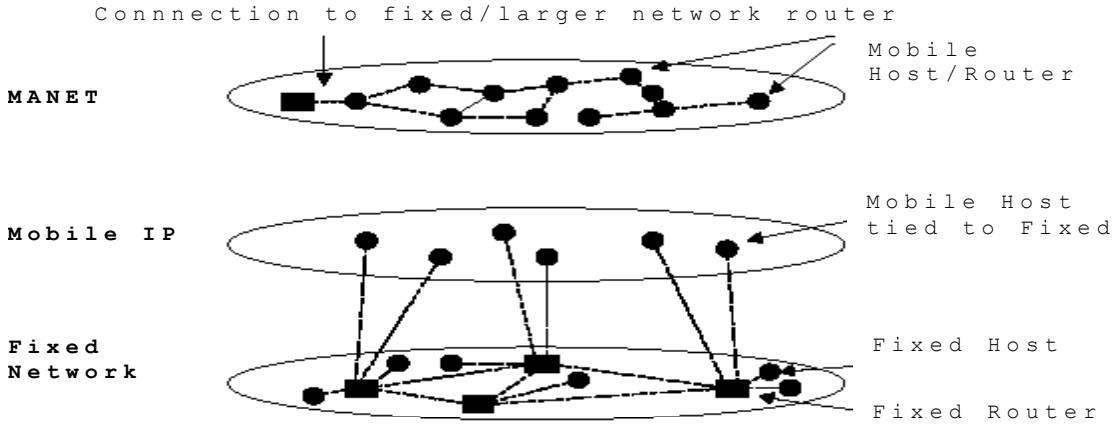


Figure 2. Network differences illustration [From: Ref. 7]

B. BENEFIT

The benefit of exploring MANET routing protocols is to identify a method of extending the range of communications on the battlefield. Forces constantly find themselves out of radio range of a major relay station and hence cut off from communicating to vital players. MANET routing protocol professes the ability for individual nodes to route for each other. This ability for nodes to route for each other is very appealing for today's networking operations and can be extended by using UAV's as routing nodes. These UAV's could serve as routers or bridges to other ad hoc networks, or to an existing networked infrastructure. The MANET Working Group is currently considering several protocols, for adoption. The MANET Working Group is a chartered working group within the Internet Engineering Task Force (IETF) to investigate and develop candidate standard Internet routing support for mobile, wireless IP autonomous segments.

IV. MODELING APPROACH

In order to create an OPNET model for the conceptual UAV network, I first researched several MANET routing protocols that were developed for OPNET simulation. Once I narrowed down the routing protocols (based on their use in a Navy/Marine Corps environment), I attempted to create and run OPNET simulations for the UAV network.

I examined the following reactive and reactive/proactive routing protocols: 1) Ad Hoc On-Demand Distance Vector routing protocol (**AODV**), 2) Dynamic Source Routing protocol (**DSR**), and 3) Zone Routing Protocol (**ZRP**). Proactive protocols continuously update the route within a network in order for quick delivery of information: this cuts down on the time required to locate a route. Reactive protocols look for routing information only on demand: this cuts down on routing overhead, especially when the network is constantly changing. Chapters V, VI, and VII detail my modeling attempts and recommendations.

THIS PAGE INTENTIONALLY LEFT BLANK

V. AD HOC ON-DEMAND DISTANCE-VECTOR PROTOCOL (AODV)

A. GENERAL

Charles Perkins and Elizabeth Royer described the Ad Hoc On-Demand Distance Vector (AODV) routing protocol as "providing quick and efficient route establishment between nodes desiring communication and that AODV was designed specifically for ad hoc wireless networks. It provides communication between mobile nodes with minimal control overhead and minimal route acquisition latency." [Ref. 6] This protocol offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within the ad hoc network. It uses destination sequence numbers to ensure loop freedom at all times, avoiding problems associated with classical distance vector protocols. [Ref. 7]

AODV is an improvement to the Destination Sequenced Distance Vector (DSDV) protocol. DSDV was originally based on distance-vector algorithm, but was later enhanced for mobile ad hoc networks. DSDV nodes on a network transmit packets via the routing tables that each node stores. Entries in the table are tagged with a sequence number that originated from the destination node. The route tables maintain consistency by periodic updates that each node transmits. Routing information is advertised by broadcasting packets and as topological changes are detected in the network, e.g. when nodes move in the network. [Ref. 6] AODV improves DSDV by reducing the

amount of control traffic. This is accomplished by simply minimizing the number of inquired routes. A node only creates and maintains routes that it is concerned with, instead of building a route for all possible destinations.

If a route is required, a *discovery* process is initiated. If the initiating node receives a response to its inquiry, it updates its routing table by creating an entry for the destination node. When no route is found within a given time period, the initiator node assumes that the destination node is unreachable. The discovery process is aborted and the corresponding data packets are dropped. This approach is known as *source-initiated on-demand* routing as opposed to *table-driven* routing. It is also known as *reactive* as opposed to *proactive*. One more improvement is related to route maintenance. If a link fails, the node affected immediately broadcasts an update message to other nodes that are affected. Figure 3 illustrates a route creation. The source node S initiates with a route request (RREQ) packet. The destination node sends a Route reply (RREP) packet, which travels along the reverse path. Each node receiving the RREP creates an entry for the destination node **D**. The destination sequence number and hop count are copied from the RREP itself and the next hop along this path is the last node that forwarded the RREP. [Ref. 9]

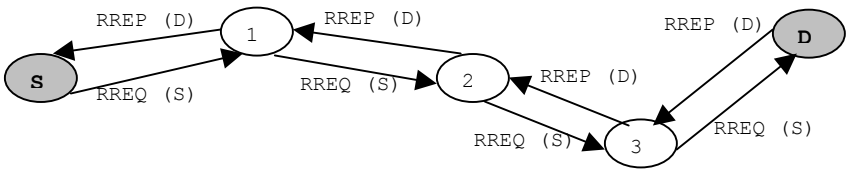


Figure 3. AODV Route Creation [After: Ref. 9]

B. SIMULATION MODELING EXPERIMENT

I examined the National Institute of Standards and Technology's (NIST) version of the AODV routing protocol that was developed for simulation using the Optimum Performance Network (OPNET) software simulation tool. NIST made the AODV model available to provide a tool for researchers and designers who need to conduct OPNET simulations of MANETs. My examination reviewed the performance of the basic subnet operations as well as the possible implementation into a more diverse network, i.e. UAV networking architecture.

The first hurdle to overcome with using the model developed by NIST was to ensure the OPNET simulation model ran correctly. NIST originally developed their model in UNIX and later made it available for windows. However, when I ran the Windows version, compilation errors occurred. This problem was fixed when Professor Bordetsky directed me to Veniamin Bourakov (a student at Stanford University). Veniamin found 2 problems in the C++ code. The problems were corrected and his comments are depicted below:

> "1. A variable was declared in the model code with name 'type'. For some reason Microsoft compiler didn't like it. It must be a reserved word of some kind for either Microsoft or for OPNET. In any case, I renamed it to 'type1'.
>
> 2. A function 'max_int' was declared. However, in the implementation part and throughout the code it was called 'max'. So, throughout the code, I renamed it 'max_int'.
>
> The Routing module was the only one giving compilation problems, so after having the above two problems fixed, the model compiled and ran."

As described in documentation from NIST, the NIST/AODV node model is tailored after the ***O****pen* ***S****ystem* ***I****nterconnection* (OSI) model. However, some layers are purposely omitted with the focus being to provide a test bed around the AODV routing implementation. Each node within the network is uniquely identified with its IP address. In the platform, the IP address is assimilated to the medium access control (MAC) address that must be indicated before the simulation compilation. Figure 4 shows the NIST/AODV node model and a description of its internal modules follow: [Ref. 9]

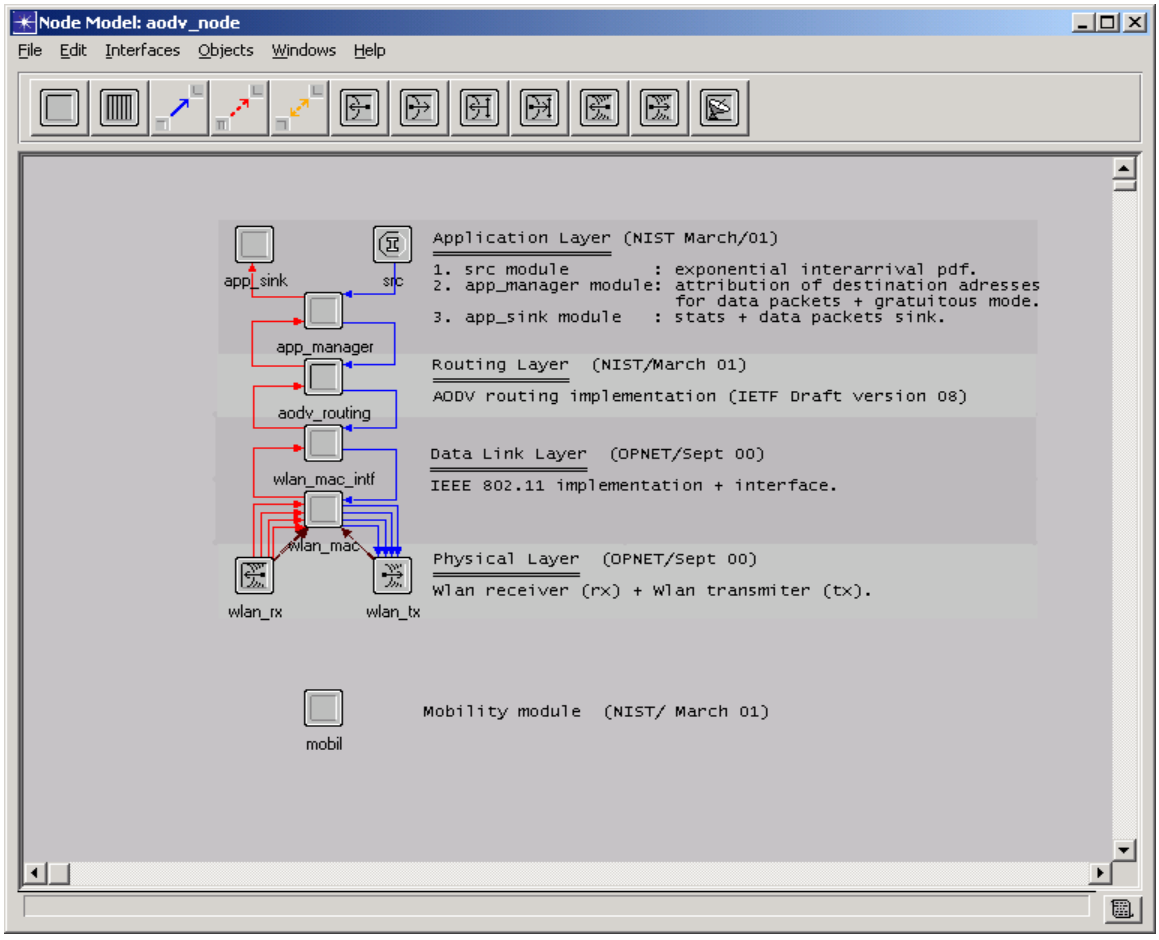


Figure 4. AODV Node Model [From: Ref. 9]

- *src* module: This is the packet source module. It generates packets according to specific packet size and inter-arrival distributions. Once generated, packets are sent to the immediate lower layer (app_manager).

- *app_manager* module: The application manager module sets a random destination address to the incoming packet and generates a service request primitive to the routing layer in the form of an Internal Communication Interface (ICI). Along with the ICI (an interface which allows two processes to exchange a user-defined information), the just received packet is sent the aodv_routing module.

- *aodv_routing* module: This module receives the packet from the application layer and executes the AODV routing algorithm as described in the previous section.

- *wlan_mac_intf* module (provided by OPNET): This module interfaces the lower layer module. It receives the packet from the aodv_routing module and hands it over to wlan_mac module and vice-versa.

- *wlan_mac* module (provided by OPNET): This module is an implementation of the **IEEE 802.11** standard MAC protocol. Some modifications were added to the original model to enable some sort of interaction with the upper layers (especially with the *aodv_routing* process). For instance, upon transmission failure, the current module hands over an ICI to the upper layers indicating the IP address of the unreachable node.

- *wlan_rx + wlan_tx* modules: These modules are implementations of the IEEE 802.11 standard *physical layer* specifications.

- *mobility* module: This mobile performs the movement of the current node by changing its position periodically according to the actual movement scheme.

The simulation was based on 18 wireless LAN based stations in the ad hoc network configuration (see Figure 5). A node's movement was bounded to a rectangular area [700m x 1000m]. This mobility scheme is very limited and is activated by setting the MOBILITY attribute (node level) to "Enabled". The movement is a sequence of discrete events and no acceleration is possible.

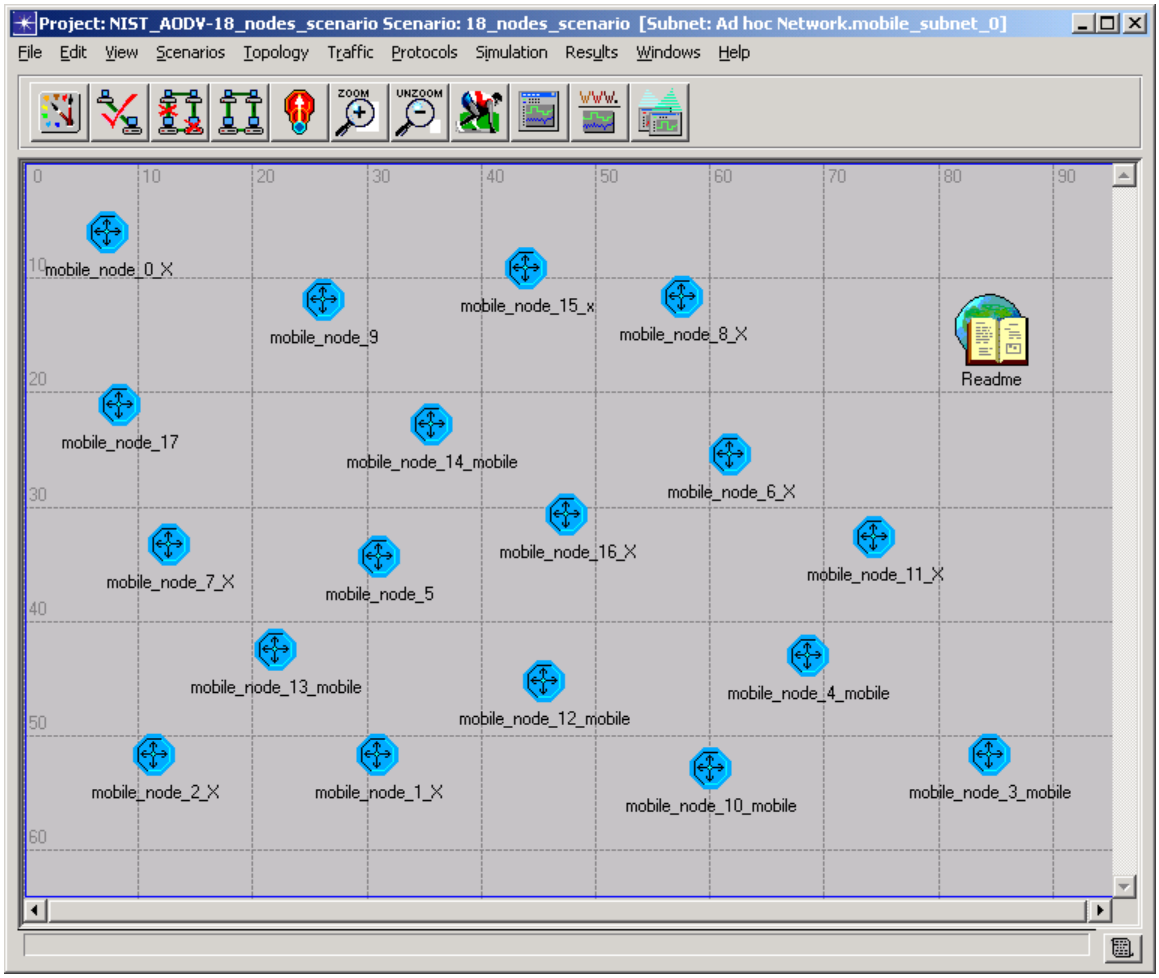


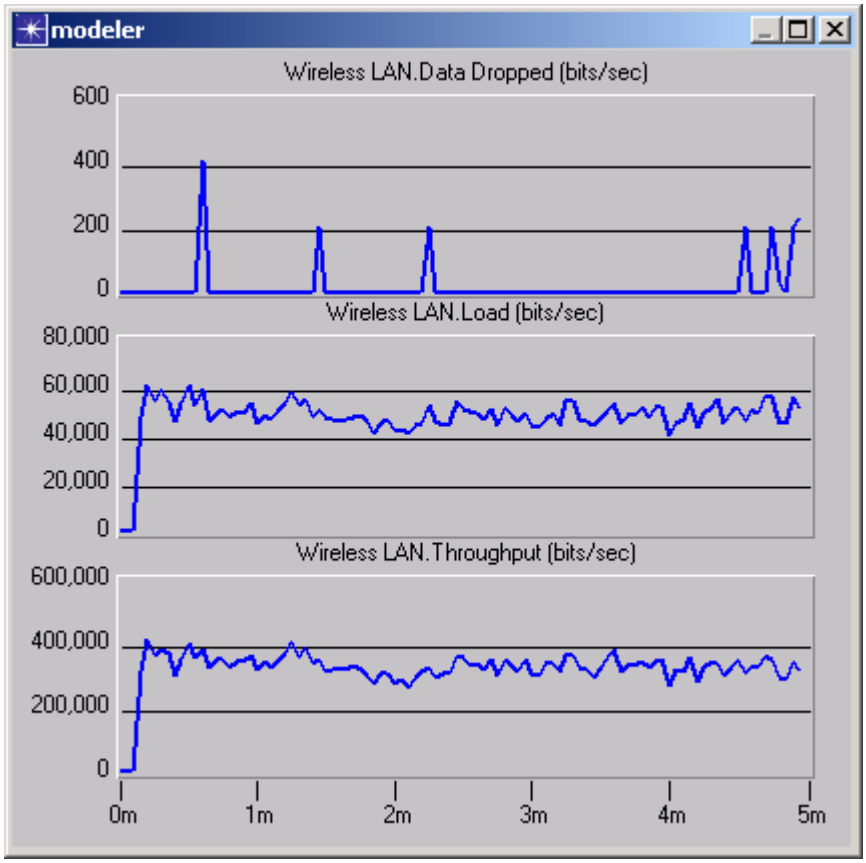
Figure 5. NIST/AODV 18 nodes scenario

Packets were generated and destined for a specific node. I chose this setup in order to measure the data being received and sent by each node. Packet generation is determined by the INTERLOCUTOR attribute and can be set to:

- "None - the node remains silent (but still performs routing function) during the simulation time.
- Multiple - node may sequentially converse with multiple nodes (each time a packet is received at the app_manager from the source, a destination is randomly computed and attributed to it before it is sent to the routing layer).
- Mono-interlocutor – you can indicate an address in the sub-network. All packets generated at the source are destined for the specified node." [Ref. 9]

C. RESULTS

Results of the scenario are depicted in Figure 6. This scenario had a simulation time of 300 seconds and was created to determine the standard capabilities of the AODV model. As the figure suggests, at any specific time the maximum data dropped compared to the total load was only about .006%. These results are terrific! But, we must remember that I only used 18 nodes that were directing generated traffic to only one other node. At this point, the intent was to determine if the AODV model simulation ran correctly for future studies in building a UAV ad hoc network.



Data Dropped - The total size of higher layer data packets (in bits/sec) dropped by all the WLAN MACs in the network due to:

a) the overflow of higher layer buffer, or

b) failure of all retransmissions until retry limit.

Load - Represents the total load (in bits/sec) submitted to wireless LAN layers by all other higher layers in all WLAN nodes of the network.

Throughput - Represents the total number of bits (in bits/sec) forwarded from wireless LAN layers to higher layers in all WLAN nodes of the network.

Figure 6. AODV simulation results

Other studies have demonstrated that as the network becomes larger and multicast operations are put into place, the efficiency is decreased. When nodes move slow, the performance is between 87% and 97%. As the node's movement increases, the smaller network outperforms the larger network by a considerable margin. [Ref. 6]

D. FINDINGS

Now that I had determined that the AODV OPNET model was a viable protocol for further testing, my next step was to connect the sub-network to a modeled communications UAV. This UAV would eventually connect the sub-network to other modeled ad hoc or fixed networks. Locating a gateway-type model created for OPENT simulations on a Windows platform,

proved to be non-productive. None of my resources had ventured to the next step of creating such a gateway. In my estimate, the creation of this model would take months of programming hours. When such a gateway is developed, the below information should be considered:

- The modeling of the communications UAV requires an OPNET router model that bridges independent ad hoc routing protocol networks, as well as, bridging ad hoc routing networks with networks that use more conventional routing protocols, i.e. OSPF, BRP, etc. For the AODV model, my researched determined that such a router model must be mutually reachable by a single hop for all participants wishing to transmit outside their respective subnet.
- Routes to the AODV subnet have to be assigned a destination sequence number and one of the nodes in the AODV subnet would be responsible for creating and managing the sequence number. This node would be labeled the *subnet leader*, and must be considered the default router for all subnet nodes. [Ref. 6]

This restriction of all nodes located within one hop of a single router limits the desired characteristics of the sought after ad hoc network. The intent of the conceptual UAV MANET, is that the nodes are not tied to a single routing source, but are able to rely on each other for transmission or forwarding of data. The previous mentioned limitation of a single hop, plus the fact that a *subnet leader* model for a Windows platform had not been developed for OPNET modeling, forced me to research another protocol for study. The next MANET routing protocol for study would be the Dynamic Source Routing (DSR) protocol.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. DYNAMIC SOURCE ROUTING PROTOCOL (DSR)

A. GENERAL

The Dynamic Source Routing protocol (DSR) was specifically designed for multihop wireless ad hoc networks. There are two mechanisms that work together to allow DSR to be completely self-organizing and self-configuring. These mechanisms are Route Discovery and Route Maintenance. Each node maintains a route cache of learned routes. If a route is unknown, the node uses the route discovery mechanism to obtain the route. The route maintenance mechanism is used in each operation to verify the existence of a route. [Ref. 6] DSR Route Discovery example is illustrated in Figure 7.

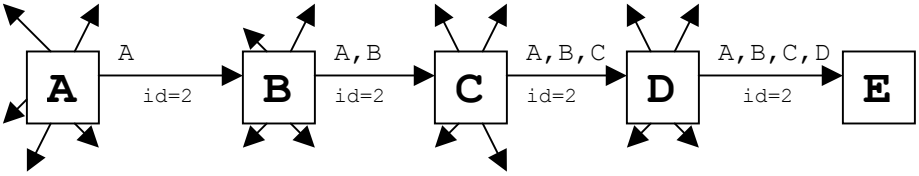


Figure 7. Route Discovery example [From: Ref. 6]

When Node **A** originates a new packet destined for Node **E**, it broadcasts a single hop ROUTE REQUEST (RREQ) message to nodes in transmission range. This message identifies the originator, the destination, contains a unique request ID, and contains a record listing the address of each intermediate node. When a different node receives an RREQ, it checks to determine if it is the intended node. If not, it appends its address to the route record in the RREQ and broadcasts a single message using the same request ID. If it is the intended node, a ROUTE REPLY (RREP) is sent to the initiator (in this case, back to node **A**) along a route

that might be obtained in the cache of Node **E** or by performing a Route Discovery.

DSR nodes are required to confirm that a packet has been received. The packet is retransmitted a predetermined number of times until confirmation of receipt is received. If no receipt confirmation is received, the node returns a ROUTE ERROR (RERR) that identifies that the link to the next node on the route is broken. DSR Route Maintenance example is shown in Figure 8. Node **A** originates a packet destined for Node **E** along a known route. Each node must return a confirmation receipt. In the example, the confirmation receipt is not received from Node **D**, therefore Node **C** returns a RERR for the link between Nodes **C** and **D**. All nodes update their route cache and Node **A** looks for another route that might be stored in its route cache from an earlier Route Discovery.

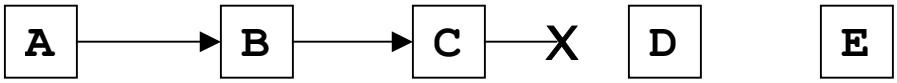


Figure 8. Route Maintenance example [From: Ref. 8]

DSR can support seamless routing as depicted with the UAV network illustration in Figure 9. This is accomplished through DSR's logical addressing model. With the use of conventional IP addressing, each ad hoc sub-network has an associated address. Each node in a particular sub-network treats that sub-network's address as its home address for all communications within the network. After the local sub-network address is assigned, each node assigns a unique *interface index* to any of the other networks to which it may communicate. [Ref. 6]

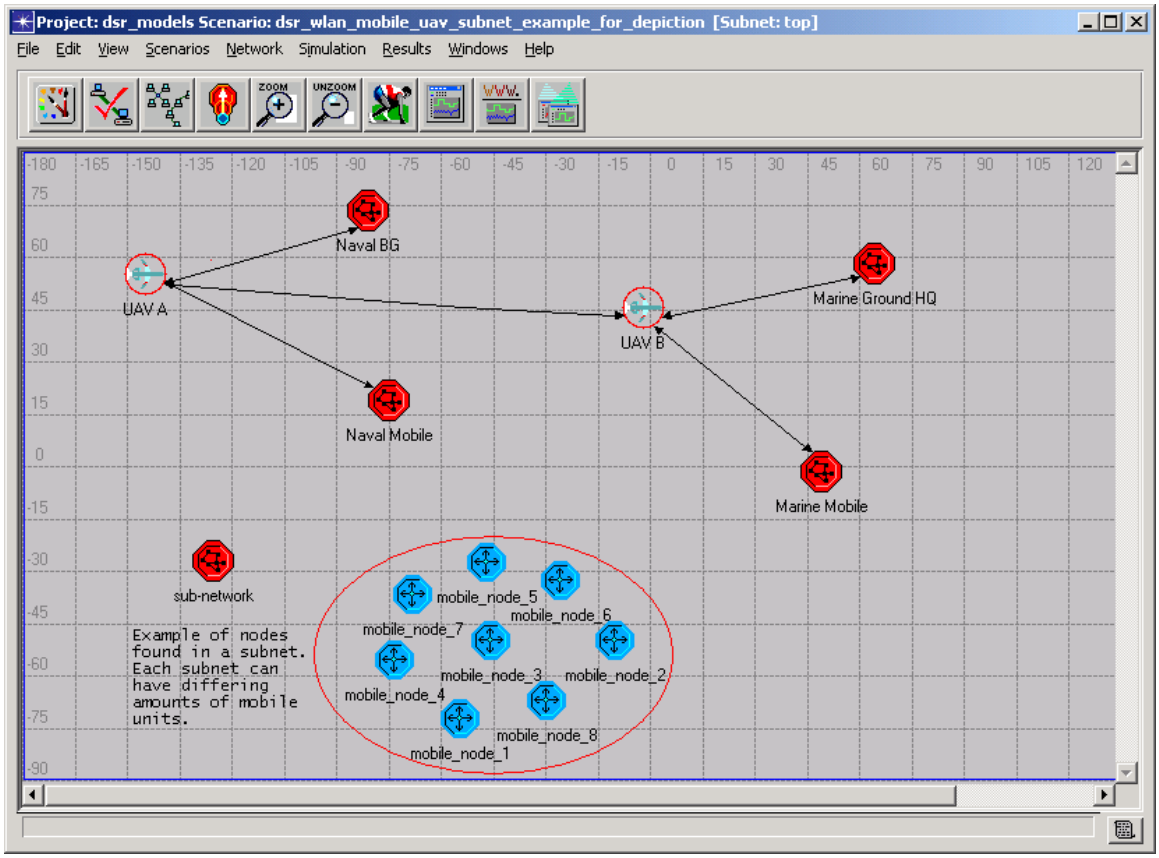


Figure 9. UAV routing to sub-networks

Based on DSR's acclaimed capabilities, it is definitely an ideal candidate for study in the extended communications battlefield using UAVs. In the military setting, some nodes will be equipped with the same type of low power transmission equipment and some can be equipped with equipment that is more powerful and capable of interfacing with a longer-range wireless network. These more powerful nodes are ideal for connecting sub-networks. This is the premise behind using a UAV. The UAV is capable of carrying more powerful equipment, enabling it to reach and connect several sub-networks.

B. SIMULATION MODELING EXPERIMENT

Again, I obtained an OPNET simulation model from NIST for evaluating DSR. NIST's DSR model was produced in the fashion of the OSI model. The model was stacked into processes and is shown in Figure 10:

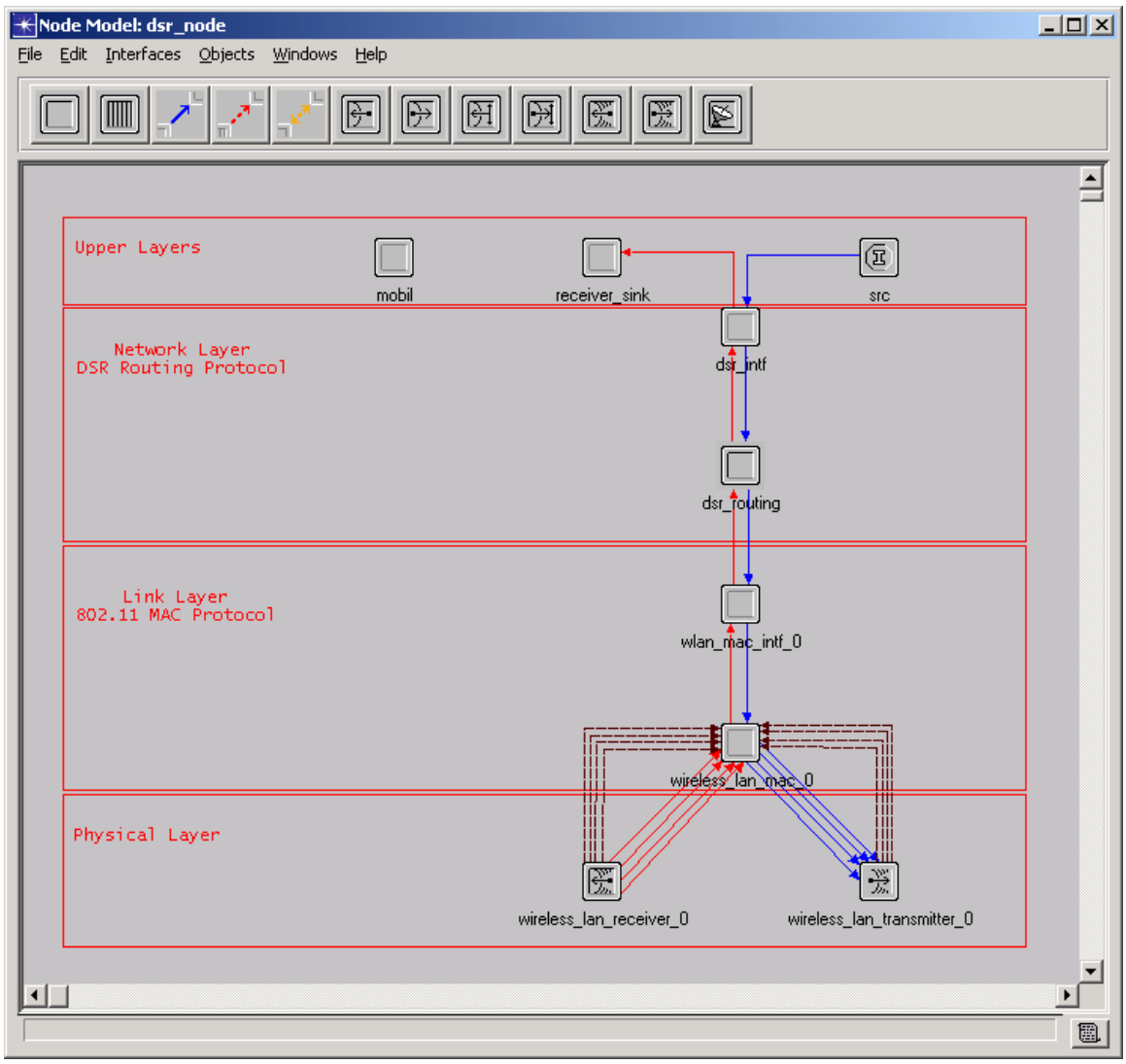


Figure 10. NIST's DSR model [After Ref. 9]

The description of each layer of the DSR node model is outlined below: [Ref. 10]

- The physical layer is composed of a transmitter and a receiver that was developed by OPNET.

- The link layer used in the model is the OPNET 802.11 model with some small modifications that link this MAC layer with the DSR routing layer, i.e. sending acknowledgement and error messages, addition of the promiscuous mode, and debugging errors to the node's mobility. This layer is divided in two processes. The first process (wireless_lan_mac_0) is the 802.11 protocol, and the second one (wlan_mac_intf_0) is an interface with the upper layer.

- The network layer contains the DSR routing process and is the core of the model. This layer is also divided into two processes, the routing module and the upper layer interface.

- The upper layers are composed of three processes. The first is the source (src) and is an OPNET process that generates data packet traffic. The receiver is a sink that just destroys the packet after reception and processing. The third is the mobile (mobil) process. The 'mobil' process is charged with mobility of the node. The mobility model used in simulations is called billiard mobility. This model has each node choose a random direction that is will follow at a constant speed. Upon reaching the network boundaries it rebounds to a new random direction.

C. RESULTS

In order to compare results of DSR to AODV, I collected the same statistical information. Again, at this time, it was my intent to determine if the DSR model simulation ran correctly for future studies in building a UAV ad hoc network. The results were just as amazing as the results of AODV, however I only used 16 nodes in this single sub-network simulation. Figure 11 suggests, at any

specific time the maximum data dropped compared to the total load was only about .003%. Other studies evaluated the packet delivery of DSR and determined the success rate of packet delivery to be around 99.5 % and routing overhead to only be .001 % [Ref. 8].

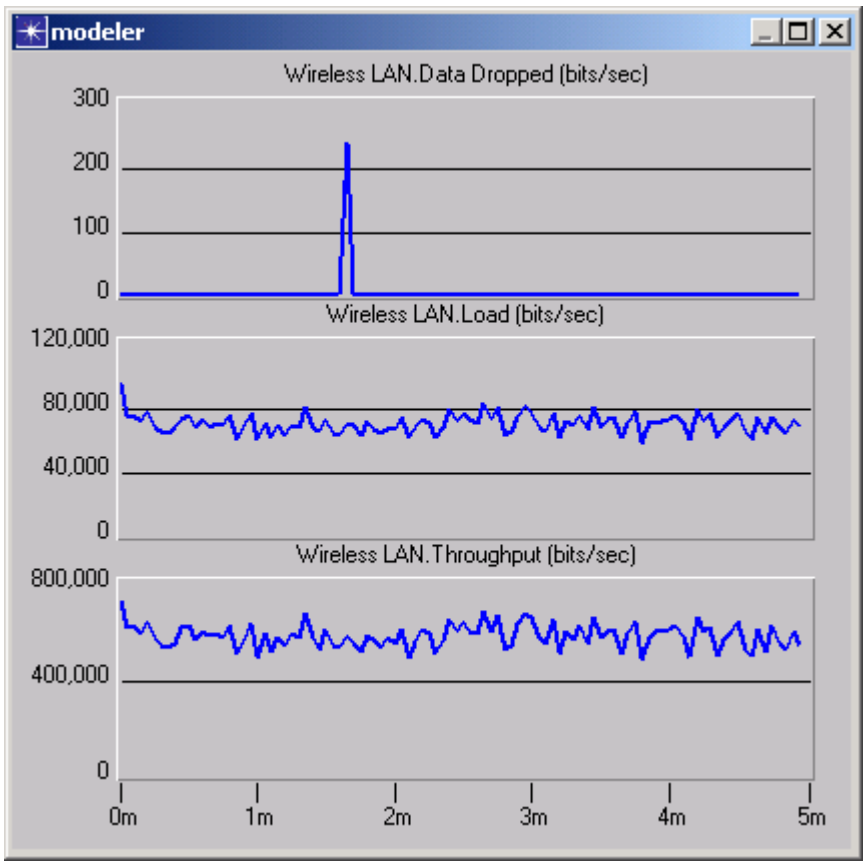


Figure 11. DSR simulation results

D. FINDINGS

Now that I had a working model, I researched building the UAV extended network using NIST's DSR simulation model. Figure 9, depicted the OPNET model that was created using DSR. I first tried to route traffic from one node to the other using standard OPNET routing protocols. This did not work. The simulation ran correctly, however, traffic was

not routed from one subnet to the other. I then checked the reference material for the NIST DSR model. The material stated, "We did not implement any IP idea, concept or mechanism in our model. The reason is that our goal is to evaluate the DSR concept and mechanism, and not its IP implementation." [Ref. 9] As I described earlier in this section, in order for the DSR network interface function (i.e. gateway) to work correctly there must be IP addressing involved. Again, as with AODV, I was faced with the fact that a gateway-type model for OPNET simulation had not been developed.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. ZONE ROUTING PROTOCOL (ZRP)

A. GENERAL

The last MANET routing protocol studied was the Zone Routing Protocol (ZRP). Zygument J. Haas and Marc R. Pearlman of Cornell University introduced ZRP as a protocol that fits in a special class of reconfigurable wireless networks (RWNs). RWNs are ad hoc networks that do not rely on pre-existing networks. The nodes in an RWN dynamically join and leave without warning. Their scheme proposes that ZRP will dynamically adjust itself to different operational conditions based on a parameter in the protocol labeled the zone radius. The zone radius is defined by the amount of hops from source node. Therefore, a node's routing zone is the collection of nodes whose minimum distance from that source node is no greater than the zone radius. [Ref. 6]

ZRP is a hybrid protocol that uses a reactive and proactive routing scheme. The proactive procedure, Intrazone Routing Protocol (IARP), is limited to the source node's local neighborhood (routing zone). While the reactive protocol, Interzone Routing Protocol (IERP), is responsible for discovering routes to destinations beyond the source node's routing zone. Figure 12 shows an example of each route discover procedure. Source **S** looks for the destination node using IARP, its routing zone is limited to 2 hops. If the destination node is not found, then **S** discovers the destination node using IERP. This routing scheme quickly locates local neighborhood nodes, while limiting the routing overhead of the entire global network.

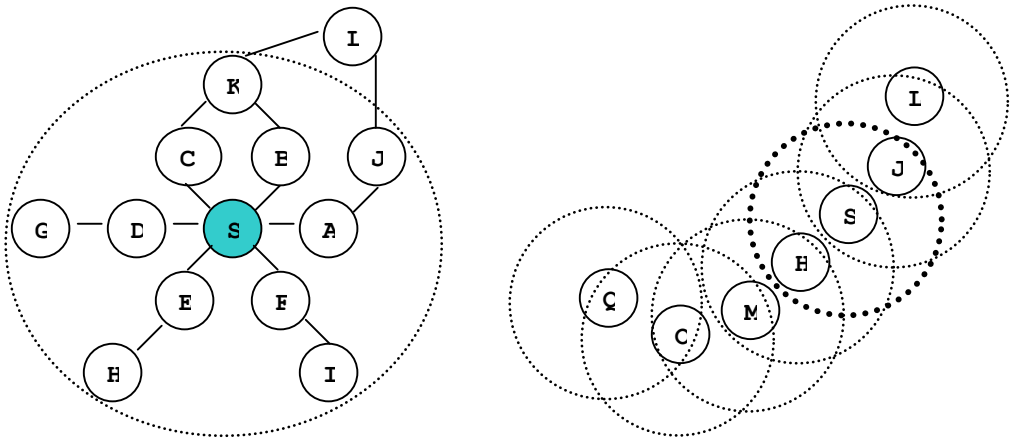


Figure 12. ZRP's IARP and IERP operations [After Ref. 5]

B. SIMULATION MODELING EXPERIMENT

I obtained an OPNET simulation model for ZRP from Cornell University's web site sponsored by Professor Haas. Figure 13 illustrates the ZRP model developed for OPNET simulation. Brief descriptions of the ZRP modules proceed and follow the figure: [Ref. 11]

- The routing node is the cornerstone of the ZRP model's routing performance. Once traffic leaves routing, it is sent to a routing protocol for handling.
- IERP and Border Routing Protocol (BRP) handle out of zone routing, while IARP handles in-zone routing.
- The beacon and delivery module were included to provide an ideal MAC behavior.
- The app module initiates and controls traffic behavior.
- *Tx_simple* and *rx_simple* modules model the transceiver pipeline built by OPNET. OPNET's transceiver pipeline attributes include: transmission delay, link closure (LOS), channel match, transmitter antenna gain, propagation delay, receiver antenna gain, received power, background noise, interference noise, signal-to-

noise ratio (SNR), bit error rate (BER), error allocation, and error correction. However, in order to simplify the model the developer bypassed these attributes and only considered distance loss.

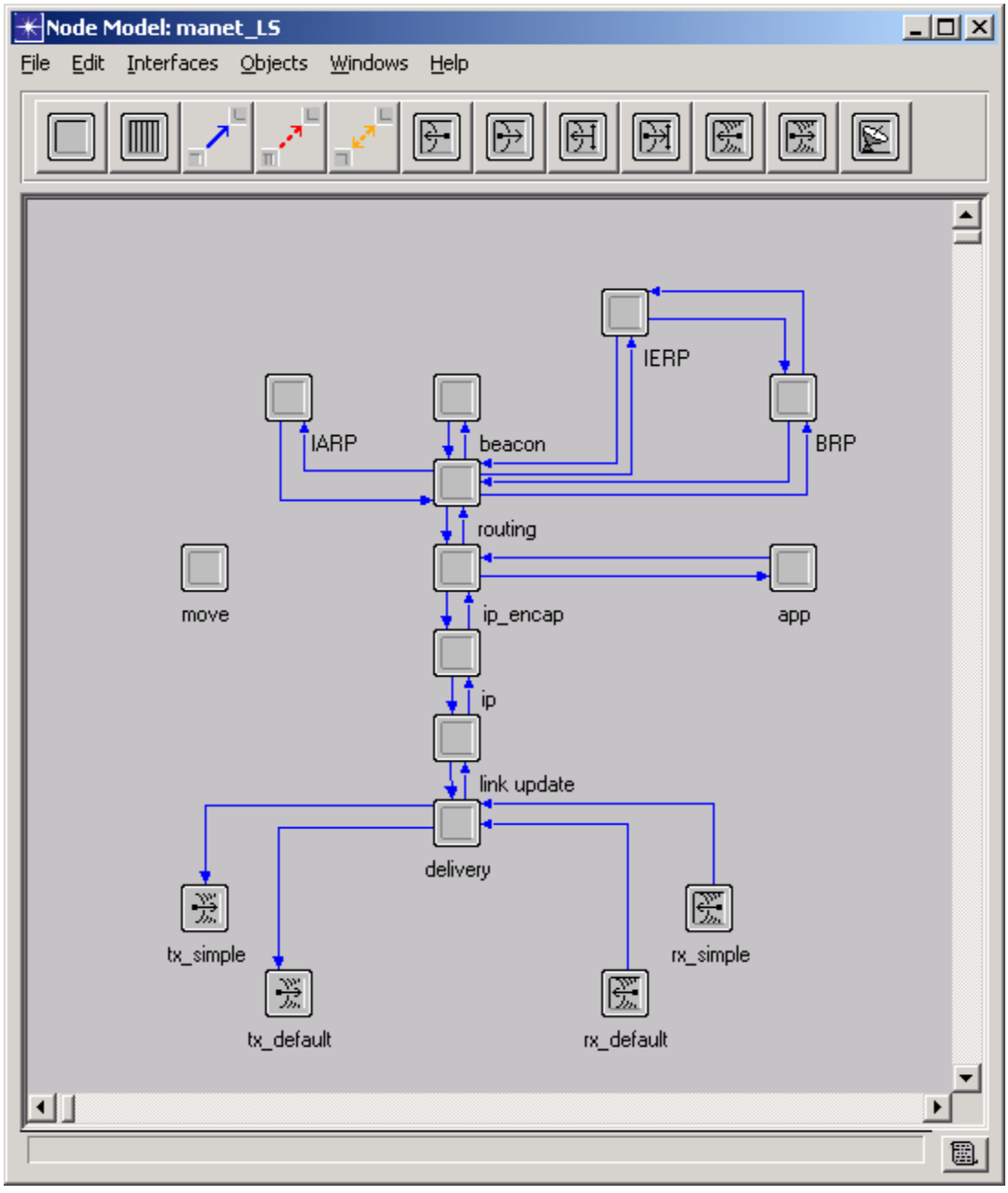


Figure 13. ZRP OPNET model

- *Tx_default* and *rx_default* modules were created for future modeling when incorporating OPNET's pipeline attributes. The developer mentioned that quite a bit of coding would be required to incorporate this feature. The transceiver is only affected by distance loss.
- Move module control the movement of the node. It moves at a designated speed and when it encounters the boundary of the pre-designated plane it rebounds and heads in another direction.
- IP and IP_encap handle the IP packet formats.
- Link update maintains updated information about links.
- The transceiver is only affected by distance loss.

C. RESULTS AND FINDINGS

The model was originally developed using a UNIX based system and was later converted to a Windows based platform. My attempts to get the Windows version to run were futile. I again turned to my friend Veniamin Bourakov in an attempt to fix the problem. He was able to get the simulation to run based on his understanding of the code, but not to the point of being able to gather accurate statistics. I then turned to previous reports on the protocol for determining its possible use in UAV operations.

After reviewing several reports, I decided that ZRP was just as good of a candidate, if not better, for UAV communication operations. The ZRP OPNET simulation results from Mr. Haas and Mr. Pearlman determined that networks characterized by highly mobile nodes and very unstable routes produce less average total control traffic than purely reactive or proactive protocols. Also, a ZRP routing zone of 2 hops produces 40% less routing traffic

than flood search and more than 50% less traffic than a proactive protocol [Ref. 6].

The OPNET simulation run by Kevin Shea, NPS Thesis, also determined that ZRP is a good candidate for consideration when establishing an ad hoc network. He compared the performance ZRP using a Marine rifle platoon (32 nodes) operating in a 1 square kilometer area of operation. His conclusions showed that ZRP is able to adapt to a Marine scenario when the zone routing radius is adjusted to suit the small size of the network, but needed to be adjusted when establishing a larger network. [Ref. 11]

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. NETWORK MANAGEMENT (ADDITIONAL ISSUES)

A. INTRODUCTION

Several factors must be considered in order to build a successful network. One major factor is network management. The network management issues mentioned in this section not only relate to the proposed UAV MANET, but to any mobile infrastructure. Management of mobile nodes must address some of the same issues that arise in standard networks. Those issues include: Fault Management, Configuration Management, Accounting Management, Performance Management and Security Management. These functions are standard throughout the network management arena and have been abbreviated to the term 'FCAPS', a term used by Mr. Lundy Lewis in reference 11.

In addition to the standard FCAPS, the International Telecommunications Union – Telecommunications (ITU-T) has provided a conceptual 5-layer stack management model that follows the OSI model. ITU calls this model the Telecommunications Management Network (TMN) layers model, which is outlined below:

- Business Management - handling overall management issue such as: billing, account management and administration.
- Service Management – service provided to a customer, e.g. service contracts, trouble ticket handling, QoS, etc.
- Network Management – oversight through network monitoring and configuration.
- Element Management - provides coordination of services through management of devices, i.e. switches, routers, bridges, etc.

- Element Level Information – look at the bare elements, mapping the physical aspects of the equipment into the TMN framework.

Today the TMN concepts are used to manage networks such as: fiber-optic, distributed cellular and satellite based wireless communication systems. With the growth of the telecommunications industry, the ITU developed their model so that a single set of protocol and service specifications will be incorporated into today's fielded equipment. [Ref. 13]

B. MOBILE MANAGEMENT ISSUES

With the development of a global infrastructure, the network management focus must also be addressed in mobile networking. The how of managing a mobile network has been outlined in reference 11. I will simply highlight some of the important issues that apply to a UAV communications network. Mr. Yemini of Columbia University and Mr. Moss of Motorola Satcom, proposed that the operations management of mobile networks can be broadly put into three layers of activities: "(1) managing physical elements, ranging from components of base stations and mobile switching centers to satellites, (2) managing network functions, ranging from connectivity to routing, and (3) managing service functions, ranging from delivery of quality of service (QoS) to fraud detection." [Ref. 14] Mobile networks must apply management techniques and these techniques can be implemented through the use of management information bases (MIBs). MIBs are a component of the Simple Network Protocol (SNMP) that enable a structure (much like IP addressing) for organizing managed devices.

The major difference in managing mobile networks vice fixed networks is the physical environment. The mobile management technique must be able to handle interactions with the physical environment. This ability to manage the network in an ever changing physical environment will prove hard to accomplish. As with the UAV communications network, the physical environment will consist of stratospheric elements, mobility/speed elements, weather related elements, etc. Successful management will be able to detect when physical elements will hinder operations and then be able to devise a network management scheme that will minimize these effects.

For the UAV communications network, management software must be developed that can detect and isolate network physical problems, while recommending a possible solution. For instance, if networking UAV's are not be able to provide WAN communications because of weather or other operational issues, the network management system must be able to look for other routes. An alternate course of action could be via the use of satellites that are linked to a high power ground station within each of the sub-networks.

Another disruption could be topology changes. Routing tables must be updated constantly and hopefully at the expense of minimal overhead. This is resolved by insuring that appropriate routing protocols are used for the networks. As discussed earlier, several MANET protocols are being considered, but for military UAV operations the protocol must be responsive to rapid-deployable type operations. Also, management software must be developed to

interact with these routing protocols. This software will be able to intervene and reconfigure operational parameters, or routing information.

A lot of the aforementioned management functions (TMN/ FCAP) can be incorporated into the node that acts as a gateway to other sub-networks. For this research, that gateway would be the UAV or as a back up it would be the designated back-up gateway (high power ground node) within each sub-network. Conclusions deduced by Mr. Yemini and Mr. Moss are directly related to the problems facing UAV communications network management and are outlined below: [Ref. 14]

- Mobile networks give rise to management problems that cannot be resolved simply by extending current management technology.
- Handling of FCAPS problems will be vital.
- Management technologies must be created that monitor the traffic flow of mobile networks.
- As mobile networks increase in size, management technologies will be vital to effective operations.

IX. SECURITY RISKS (ADDITIONAL ISSUES)

Security is essential to the operations of any organizations. Without adequate security, all attempts at being successful will fail. There is no exception in the case of a network of UAV's that uses MANET routing protocols. Because of the wireless nature of this network, it is more prone to security risks than a fixed infrastructure. In designing this network, considerable consideration must be given to security concerns. In an attempt to explore new approaches to securing MANET's, Professor Zygmunt J. Haas and Lidong Zhou published a paper entitled, 'Securing Ad Hoc Networks'. In the paper, they outlined some security issues and possible solutions to those issues. The below quote summarizes their initial security concerns:

> "In most routing protocols, routers exchange information on the topology of the network in order to establish routes between nodes. Such information could become a target for malicious adversaries…
>
> There are two sources of threats to routing protocols…
>
> The first comes from external attackers. By injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce excessive traffic load into the network…
>
> The second and also the more severe kind of threat comes from compromised nodes, which might advertise incorrect routing information to other nodes." [Ref. 15]

Professor Haas and Zhou deduced that protection against the first kind of threat could be accomplished through current cryptographic techniques, but the second threat requires a more dynamic approach. As a matter of fact, the very properties of ad hoc networking can aid in going around compromised nodes. This 'go around' is simply the routing protocols updating mechanisms; when there are a sufficient amount of non-compromised nodes. In the routing mechanisms, outdated routing information is frequently updated; therefore compromised nodes could be considered as outdated information. Another proposed solution to this threat is through the use of a key management system designed for ad hoc networks. In their paper they discussed their notion of a 'threshold cryptographic' system, but that is beyond the scope of this thesis. [Ref. 15]

In general, several security levels must be initiated before establishing a wireless network for military operations. Some researchers and authorities have raised concerns and even proposed solutions. I too wanted to ensure that security issues were considered before developing a UAV communications network. This thesis is not intended to delve into the various security concerns but to highlight the importance for consideration. Several books, papers, and even NPS theses have been published in the area of wireless communications vulnerabilities; therefore, I recommend that those types of publications be viewed when creating security measures for MANETs.

X. CONCLUSION AND RECOMMENDATIONS

A. CONCLUSIONS

This thesis represents the initial phase of research for determining a routing model for a UAV communications MANET. The results are based on analysis of three MANET routing protocols and extensive research concerning additional issues. The results indicate that further development of OPNET MANET routing protocol models is needed in order to sufficiently model the proposed UAV MANET. Without this development, OPNET simulation research of networks using MANET protocols will be limited and inefficient.

The limited simulation results indicate that AODV, DSR, and ZRP are protocols that show considerable potential. These results indicate that the protocols' performance were well within acceptable parameters for mobile ad hoc wireless communications. Also, other studies indicate that these protocols only need to be incorporated into a live network for continued development.

B. RECOMMENDATIONS

For continued research in OPNET modeling of UAV communication MANETs, I recommend that a network interface type model (e.g. gateway) be developed for studying the various routing protocols'. Focus should be directed towards sub-network to sub-network interactions. Despite the fact that the OPNET simulation models have not been completely developed for WAN operations, I recommend the continued use of OPNET. OPNET's ability to model and

collect data during all phases of simulation study is unsurpassed.

Three routing protocols were considered in this thesis, but other ad hoc routing protocols are under consideration by the IETF. My preliminary research concluded that AODV, DSR, and ZRP deserved the most attention for military type operations. Of the three, I recommend that DSR and ZRP receive the first priority in further testing. I make this recommendation based on the fact that, DSR and ZRP are more compatible with Navy/Marine Corps type operations. These recommendations are strictly the views of the author and intended to aid future modeling developers and Navy/Marine Corps researchers.

LIST OF REFERENCES

1. Cebrowski, Arthur K., and John J. Garstka. "Network-Centric Warfare: Its Origin and Future." U. S. Naval Institute Proceedings 124, no. 1(January 1998): 28-35.

2. United States Marine Corps. Strategy 21. November 2000.

3. United States Navy and Marine Corps. Forward From the Sea. March 1997.

4. United States Air Force. Global Hawk Information for Airborne Communications Node Solicitation Brief. 29 Aug 97.

5. Ferguson, Charles R., and Harbold Douglas A. " High Altitude Long Endurance (HALE) Platforms for Tactical Wireless Communications and Sensor use in Military Operations." Thesis, Naval Postgraduate School, September 2001.

6. Perkins, Charles E. Ad Hoc Networking. Addison-Wesley, New York, NY, 2001.

7. Theriot, Tyrone P. "Simulation and Performance Analysis of the Ad Hoc On-Demand Distance Vector Routing Protocol for Tactical Mobile Ad Hoc Network." Thesis, Naval Postgraduate School, December 2000.

8. Das, Samir R., Perkins, Charles E., and Royer, Elizabeth M. " The Ad-hoc On-Demand Distance Vector Routing Protocol (AODV) for Ad Hoc Networks." Internet Draft, draft-ietf-manet-aodv-10.txt, January 2002.

9. Guemari, Lyes. "An OPNET model implementation for Ad-hoc On demand Distance Vector Routing Protocol." Thesis, Information Technology Laboratory of the National Institute of Standards and Technology, August 20, 2001.

10. National Institute of Standards and Technology. AODV OPNET Model Simulation and Notes. July 2001.

11. Shea, Kevin M. "Simulation and Performance Analysis of the Zone Routing Protocol for Tactical Mobile Ad Hoc Networks." Thesis, Naval Postgraduate School, September 2000.

12. Lewis, Lundy. Managing Business and Service Networks. Kluwer Academic/Plenum Publishers, New York, NY, 2001

13. Telecommunications Management Networks (TMN) http://www.cellsoft.de/telecom/tmn.htm

14. Aidarous, Salah, and Plevyak, Thomas. Telecommunications Network Management. The Institute of Electrical and Electronics Engineer, Inc., New York, NY, 1998

15. Haas, Zygmunt J., and Zhou, Lidong. "Securing Ad Hoc Networks." Paper Cornell University, Itaca, New York, NY.

16. Corson, Scott S., and Macker, J. "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations." RFC 2501, January 1999.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

4. Director, Training and Education, MCCDC, Code C46
   Quantico, Virginia

5. Director, Marine Corps Research Center, MCCDC, Code C40RC
   Quantico, Virginia

6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, California

7. Professor Alex Bordetsky, Code
   Naval Postgraduate School
   Monterey, California

8. Chairman, C4I Academic Group
   Naval Postgraduate School
   Monterey, California

9. Professor Isaac Kaminer, Code
   Naval Postgraduate School
   Monterey, California